UNISYS

Distributed Processing Middleware

ODBC Access for ClearPath OS 2200 Administrator User's Guide

ClearPath OS 2200 Release 14.0

February 2013 7862 5746–004

NO WARRANTIES OF ANY NATURE ARE EXTENDED BY THIS DOCUMENT. Any product or related information described herein is only furnished pursuant and subject to the terms and conditions of a duly executed agreement to purchase or lease equipment or to license software. The only warranties made by Unisys, if any, with respect to the products described in this document are set forth in such agreement. Unisys cannot accept any financial or other responsibility that may be the result of your use of the information in this document or software material, including direct, special, or consequential damages.

You should be very careful to ensure that the use of this information and/or software material complies with the laws, rules, and regulations of the jurisdictions with respect to which it is used.

The information contained herein is subject to change without notice. Revisions may be issued to advise of such changes and/or additions.

Notice to U.S. Government End Users: This is commercial computer software or hardware documentation developed at private expense. Use, reproduction, or disclosure by the Government is subject to the terms of Unisys standard commercial license for the products, and where applicable, the restricted/limited rights provisions of the contract data rights clauses.

Unisys and ClearPath are registered trademarks of Unisys Corporation in the United States and other countries.
All other brands and products referenced in this document are acknowledged to be the trademarks or registered trademarks of their respective holders.

Contents

Section 1. Introduction

1.1. Overview 1–1
1.2. Documentation Updates 1–1
1.3. Documentation Conventions 1–1
1.4. System Requirements 1–2
1.5. Product Description 1–3
1.5.1. Installation 1–4
1.5.2. Viewing Remote Databases 1–5

Section 2. User Interface

2.1. Overview 2–1
2.2. Menus 2–1
2.2.1. File Menu 2–1
2.2.2. View Menu 2–2
2.2.3. Server Admin Menu 2–2
2.2.4. Host Admin Menu 2–2
2.2.5. Database Admin Menu 2–2
2.2.6. User Admin Menu 2–4
2.3. The Tool Bar 2–4
2.3.1. Save 2–4
2.3.2. New 2–5
2.3.3. Modify 2–5
2.3.4. Remove 2–5
2.3.5. Create View 2–5
2.3.6. Replay View 2–5
2.3.7. Create Synonym 2–5
2.3.8. Refresh 2–5
2.4. Tree View 2–6
2.4.1. ODBC Access Node 2–6
2.4.2. Servers Node 2–6
2.4.3. Versions Node 2–7
2.4.4. Installations Node 2–8
2.4.5. Databases Node 2–9
2.4.6. OS Host Node 2–12
2.4.7. Tables Node 2–12
2.4.8. Columns Node 2–13
2.4.9. Indices Node 2–14
2.4.10. Tables/Users Node 2–14
2.4.11. Views Node 2–16
2.4.12. Synonyms Node 2–17
2.4.13. OS Hosts 2–18

2.4.14. Configuration Node 2–19
2.4.15. Users Node 2–21
2.4.16. All Users Node 2–22
2.5. Security Types 2–25
2.5.1. Data Access Security 2–26
2.5.2. Windows (Impersonate) 2–26
2.5.3. Windows (Do Not Impersonate) 2–27
2.5.4. Windows Advanced Options 2–28
2.5.5. Preauthorized 2–28
2.5.6. Active Users Node 2–29
2.5.7. Dynamic Tab 2–29
2.6. View Builder 2–30
2.6.1. View Name 2–30
2.6.2. Select Tables 2–31
2.6.3. Select Column or Expression 2–31
2.6.4. Setup Column Expression 2–32
2.6.5. Setup Condition 2–33
2.6.6. Select Conditions 2–34

Section 3. Common Procedures

3.1. Overview 3–1
3.1.1. Configuration Procedures 3–1
3.1.2. Database Procedures 3–1
3.1.3. User Procedures 3–1
3.2. Configuration Procedures 3–2
3.2.1. Add a New Windows Server 3–2
3.2.2. Add a New OS 2200 Host 3–2
3.2.3. Replace Lost Configuration Information 3–2
3.3. Database Procedures 3–3
3.3.1. Load the Catalog for a New Database 3–3
3.3.2. Reload Database/Apply External Script 3–3
3.3.3. View Table or Definitions 3–4
3.3.4. Create a New View 3–4
3.3.5. Modify a View Definition 3–4
3.3.6. Re-create a View 3–4
3.3.7. Create a New Synonym 3–5
3.3.8. Change Access Permissions 3–5
3.4. User Procedures 3–5
3.4.1. Add a New User 3–5
3.4.2. Make a User the Default User 3–5
3.4.3. Set the System's Default Authentication Method 3–6
3.4.4. Set Default Query Limits 3–6
3.4.5. Monitor an Active User 3–6
3.4.6. Stop a Runaway Query 3–7

Appendix A. Troubleshooting

A.1. Overview A–1
A.1.1. Electronic Support Services A–1

A.1.2. Unisys Support Center A–1
A.1.3. Providing Information to Technical Support A–2

Appendix B. Taking Traces

B.1. Overview B–1
B.2. Administrator Trace B–1

Index 1

Section 1
Introduction

1.1. Overview

This guide contains instructions for installing and using the ODBC Access Administrator. It is installed on the same Windows server as the ODBC Access SQL Server. In addition, it can be installed on an administrator's workstation to enable remote administration of ODBC Access.

Note: *Read the software release notes before you install or use this product.*

When the ODBC Access Windows Server is installed, the Administrator is automatically installed on the same machine. Refer to the *ODBC Access Installation and Operations Guide* for the complete configuration procedure.

1.2. Documentation Updates

This document contains all the information that was available at the time of publication. Changes identified after release of this document are included in problem list entry (PLE) 18894807. To obtain a copy of the PLE, contact your Unisys service representative or access the current PLE from the Unisys Product Support Web site:

http://www.support.unisys.com/all/ple/18894807

Note*: If you are not logged into the Product Support site, you will be asked to do so.*

1.3. Documentation Conventions

This guide uses the following documentation conventions:

- Text that appears on the screen, field names, and text entered at the system prompt on the system appear in the following type style:

  ```
  select name, base_salary, sales * commission from...
  ```

  The same type style is also used for sample code segments that are listed within this guide.

- Keys with names consisting of more than one character appear within brackets, as in [Alt] or enter. Do not type the brackets; simply press the indicated key.
- Some keyboards have a [Return] key instead of an [Enter] key. This guide uses [Enter] to indicate both.

- In this guide, when you see the [Alt] key, [Shift] key, or [Ctrl] key followed by another key, press and hold down the [Alt], [Shift], or [Ctrl] key while you press the specified key. Then release both keys. For example, [Ctrl] C means press the [Ctrl] key and the letter "C" key simultaneously.
- Within the Windows environment, there are often several ways to select an option. For example, to choose OK with the mouse, you can do any of the following:
  - Click OK with the mouse
  - Type [Alt] O
  - Press the [Enter] key (because the OK button currently has focus)

  This guide uses the term choose to indicate any of these actions, as in "Choose OK."
- The following status symbols are used throughout the guide:

  To add a server.

  To remove a server from the list.

  A connection to this database is active from this Administrator.

   The previous mapping operation on this database failed.

   The configuration information for this database was lost.

  Indicates that the view was created by the interactive View Builder and also exists in the relational catalog. It can be modified using the View Builder.

  Indicates that the view was created from another source. It exists in the relational catalog, but cannot be modified.

  Denotes the default user node.

  The view was created by the View Builder, but is not in the relational catalog.

1.4. System Requirements

- Windows XP Service Pack 3, Windows 7 Service Pack 1 (or later) or Windows 8.
- Internet Explorer 7.0 or later must be installed for ODBC Access Help to function. It must be present, but does not have to be the default browser.
- Distributed COM (DCOM) is enabled. This is the default.
- ODBC infrastructure must be installed on the machine if you intend to use ODBC Access. This is standard on Windows XP or later. Its presence can be verified by looking in the Control Panel for ODBC or in the Administrative Tools folder for Data Sources (ODBC).

  If the ODBC infrastructure is not present, install it from the Microsoft Office installation media or download and install MDAC from the Microsoft Web site.

- The system Dynamic Link Library (DLL), msvcrt.dll, requires version 6.1.8581.0 or later. On systems that do not have system file protection, the installation program determines if it is present and, if not, requests you to install it. The installation terminates the DLL after installing msvcrt.dll because the system must be restarted after installing it and before continuing with the ODBC Access installation. When the system has been restarted, start the ODBC Access installation again.

1.5. Product Description

The ODBC Access Administrator allows you to browse one or more installations of ODBC Access on your site's network from a graphical interface. You can review database definitions and configuration parameters, make configuration changes and initiate a new mapping of a new database, or regenerate an existing database mapping. It is also used to manage user authentication and privileges.

Many of the operations operate directly on the ODBC Access SQL Server and therefore require it to be available. Other operations make use of configuration files and registry settings on the local machine or a remote machine, while others execute programs on the remote machines. Remote operations require a working Windows network to function correctly. For example, to read a configuration file from a machine called "Zulu", that machine must be accessible from the machine running the ODBC Access Administrator using Microsoft's Universal Naming Convention (UNC), for example, \\Zulu\.

This release of the ODBC Access Administrator does not permit configuration of the ODBC Access OS 2200 environment file. This is accomplished through changes to the ODBC Access environment file on that platform. Refer to the *ODBC Access Installation and Operations Guide* for more details.

The Administrator creates the catalog for a database and reloads the catalog by applying the DDL scripts generated from the ODBC Access Modeller. This process is time consuming and can take several minutes to complete. Because changes do not trigger an automatic regeneration of the catalog, you need to explicitly trigger catalog regeneration. Administrator commands, which require the catalog to be rebuilt, are marked with in this guide.

The Administrator presents information within the context of a tree view similar to Windows Explorer. The root node of the tree is ODBC Access. For any one release of ODBC Access, there are two major groups of information. The first group of information covers installation parameters and database definitions, and the second group covers user information and authentication.

The following major functions can be accomplished within the installation and database group:

- Basic configuration parameters can be viewed and altered.
- Full database definitions can be viewed, including all tables, columns, indexes, views, and synonyms.

- Permissions can be set graphically instead of having to use GRANT and REVOKE statements.
- Synonyms can be created and removed graphically instead of having to use CREATE and DROP statements.
- A sophisticated graphical view builder is available.

The following major functions can be accomplished within the users and authentication group:

- Setting the type of authentication applied to each user.
- Enabling or disabling a user account.
- Setting query limits.
- Setting trace options.
- Determining which users are connected to the system.
- Terminating a long query.
- Determining how close an active user is to their defined query limits.

While the ODBC Access SQL Server or the Administrator is running, all user information is held in a protected, shared area of memory. A copy is also maintained in an encrypted file on the same machine as the ODBC Access SQL Server.

The Administrator is installed on the same Windows server as the ODBC Access SQL Server. You can install it on other Windows servers or workstations on the network, and connect it to any ODBC Access SQL Server.

For user interface information, see Section 2, “User Interface.”

1.5.1. Installation

To install the ODBC Access Administrator, perform the following steps:

1. Log on as an administrator.
2. Use the ODBC Access Windows Server installation media.
3. If the setup program does not start automatically, run setup from the root folder.
4. Select the **Administrator Only** option and follow the instructions.

Note: *If you have installed Windows Vista or later, you must right-click the setup.exe file in Windows Explorer, and select* ***Run as Administrator****. In addition, you must install the software in a directory other than Program Files.*

The following steps are recommended, but not required:

1. Use Windows Explorer to navigate to the ODBC Access Administrator folder. The default is \Program Files\Unisys\ODBCAccess\Release <number>\Administrator.
2. Select the Administrator.exe file, select Properties, select Security and then choose Permissions.
3. Add Administrator accounts that require access to the ODBC Access Administrator and remove all accounts that should not have access (or remove their Execute permission). ODBC Access administrators only execute this program.

1.5.2. Viewing Remote Databases

In order to view database definitions on a remote machine, the following conditions must be met:

- The ODBC Access installation folder on the remote machine must be accessible through a share. The share can be at any level equal to or higher than the installation folder. The built-in administrative shares, such as C$, are not sufficient.
- The installation folder and its subfolders must be accessible by the user of the Administrator. Permissions are set appropriately at the share level and the folder level.

The recommended approach is to grant access to the Data Access Administrators group at the share and folder levels. This ensures anyone who uses the Administrator can also view remote database definitions.

Section 2
User Interface

2.1. Overview

This section describes key user interface elements, such as menus specific to this product, buttons on the tool bar, and the important dialog boxes. The standard menus such as Edit, Windows, and Help are not described.

The tree view is the dominant part of the interface, where you spend most of your time.

2.2. Menus

The following menus are important user interface elements:

- File menu
- View menu
- Server admin menu
- Host admin menu
- Database admin menu
- User admin menu

2.2.1. File Menu

Save

When updating installation user information, the Update button on the dialog box updates the memory copy of the user database. Select the Save menu item to ensure information is stored immediately in the SysUsers backup file.

This is usually not required because certain operations performed by the ODBC Access SQL Server cause the information to be saved to disk and, if the ODBC Access system becomes completely idle, it is saved.

The Save operation is recommended to guard against unforeseen events such as power failures or other catastrophic system failures.

Exit

Closes all active database connections and then closes the Administrator.

2.2.2. View Menu

Properties

This option presents the Properties dialog box. The Options tab lets you set the refresh interval for viewing active connections to the ODBC Access Windows server. It is active only when a tree node subordinate to the Users node is selected.

Refresh

This option refreshes the list of users or database catalog information. When an active user is selected, the limits bars on the Dynamic tab are refreshed automatically using the refresh interval from the Properties dialog box. A manual refresh can be necessary if there is more than one instance of the Administrator connected to the same ODBC Access Windows server. Refresh shows any changes made by other administrators. The same is true of database catalog information altered by other users of the ODBC Access Administrator.

2.2.3. Server Admin Menu

New Server

This item is available only when the Servers node is selected. It adds a Windows server to the list managed by the Administrator.

Remove

This item is available only when a server is selected. It removes the Windows server from the list managed by the Administrator.

2.2.4. Host Admin Menu

New Host

This item is available only when the OS Host node is selected. It records details of a new OS 2200 host. You must add a new host before associating any databases with it.

Remove Host

This item is available only when an OS 2200 Host is selected. It removes an OS 2200 Host from the list managed by the Administrator. You can remove a host if there are no databases associated with it.

2.2.5. Database Admin Menu

New Database

This item is available only when the Databases node is selected. It loads the catalog for new database so that the ODBC Access Windows server is able to access it.

Remove Database

This item is available only when a database is selected. It removes the database from the list managed by the Administrator and renders it inaccessible to the ODBC Access Windows server.

Removing a database removes the database folder (database_name.dbs) and the relational catalog files it contains. This operation can fail if any of the catalog files are in use. They could be in use when a legitimate ODBC Access session is in progress, a failed session is still active, another application has one of the files open, or when one of the files is selected in the Windows File Explorer. In all cases, wait for the application with the lock to finish (if it is legitimate), or end it if it is not, and then try to remove the database again.

Note: *If the removal of a database fails, it is likely that the removal of some files succeeded and the database is no longer in a usable state. After determining the cause and correcting it, select Remove Database again to remove the remaining files.*

Remap Database/Apply Script

This item is available only when the Databases node is selected. It remaps an existing database.

Close Database

This item is available only when a database is selected and you are connected to that database. It closes the connection to the selected database. A database with an open connection is marked with a symbol.

Grant Permissions

This item is available only when the selected Users node is subordinate to a table, view, or synonym node. It lets you add users to the list to access that table, view, or synonym. Once added, the user node can be selected to specify the permissions in the right-hand pane.

Create View

This item is available only when the Views node is selected. It invokes the ODBC Access View Builder, which permits graphical view definitions.

Create Synonym

This item is available only when a table node or a view node is selected. You can create a public synonym for the selected table or view without knowing the SQL syntax.

Drop View

This item is available only when a view is selected. It removes the view.

Drop Synonym

This item is available only when a synonym is selected. It removes the synonym.

2.2.6. User Admin Menu

New User

This item is available only when the All Users node is selected. It permits a new ODBC Access user to be added.

Remove User

This item is available only when a user is selected. It removes an existing user's information. If the authentication method for the default user is Data Access, it prevents that user from connecting to ODBC Access.

Make Default User

This item is available only when a user is selected. It makes the selected user the default user and makes the previous default user an ordinary user. The default user is marked with a symbol. The default user can connect to ODBC Access just like any other user, but it also provides default information to the new user dialog, and it supplies the default authentication type for the system.

2.3. The Tool Bar

The following tool bar user interface elements are important:

- Save
- New
- Modify
- Remove
- Create View
- Replay View
- Create Synonym
- Refresh

2.3.1. Save

When updating installation user information, the Update button on the dialog box updates the memory copy of the user database. In order to ensure the information is stored immediately in the SysUsers backup file, select the Save button.

This is usually not required because some operations performed by the ODBC Access SQL Server cause the information to be saved to disk, and, if the ODBC Access system becomes completely idle, it is saved.

The Save operation is recommended to guard against the unforeseen, such as power failures or other catastrophic system failures.

2.3.2. New

Whenever a tree node that permits child nodes to be inserted is selected, the New button becomes available. Selecting it invokes an appropriate dialog box, depending on the context.

2.3.3. Modify

This button is available whenever a view that can be modified is selected.

2.3.4. Remove

Whenever a node that can be removed is selected, the Remove button becomes available. Selecting it removes the selected tree node.

2.3.5. Create View

This button is available when the Views node is selected. Selecting this button invokes the ODBC Access View Builder, which permits view definitions to be defined graphically.

2.3.6. Replay View

This button adds newly created views to the relational catalog.

When a view is created from within the View Builder, its definition is retained when a database is remapped, but the view is not in the relational catalog and cannot be used initially by the ODBC Access SQL Server. The mapping process creates a new relational catalog. These view definitions not currently in the relational catalog are designated with the icon.

Selecting the Views node and then the Replay View button replays all the views in this state. They are added to the relational catalog.

Selecting a specific view and the Replay View button replays that view only. It is added to the relational catalog.

2.3.7. Create Synonym

This button is available when a table or view node is selected. You can create a public synonym for the selected table or view without knowing the SQL syntax.

2.3.8. Refresh

This button refreshes the list of users or database catalog information. When an active user is selected, the limits bars on the Dynamic tab refresh automatically using the refresh interval from the Properties dialog box. A manual refresh is needed if there was more than one instance of the ODBC Access Administrator connected to the same ODBC Access Windows server. Refresh shows any changes made by other administrators. The same is true of database catalog information altered by other users of the ODBC Access Administrator.

2.4. Tree View

This topic provides links to descriptions of the major nodes on the ODBC Access Administrator tree.

2.4.1. ODBC Access Node

The ODBC Access node is the root of the tree and is the starting point for all administrative activities. Double-click this node to open it.

The following nodes display:

- ODBC Access/Servers
- ODBC Access/Servers/Versions
- ODBC Access/Servers/Versions/Installations
- ODBC Access/Servers/Versions/Installations/Databases
- ODBC Access/Servers/Versions/Installations/Databases/OS Host
- ODBC Access/Servers/Versions/Installations/Databases/Tables
- ODBC Access/Servers/Versions/Installations/Databases/Tables/Columns
- ODBC Access/Servers/Versions/Installations/Databases/Tables/Users
- ODBC Access/Servers/Versions/Installations/Databases/Tables/Indices
- ODBC Access/Servers/Versions/Installations/Databases/Views
- ODBC Access/Servers/Versions/Installations/Databases/Synonyms
- ODBC Access/Servers/Versions/Installations/OS Hosts
- ODBC Access/Servers/Versions/Installations/Configuration
- ODBC Access/Servers/Versions/Users
- ODBC Access/Servers/Versions/Users/Active Users
- ODBC Access/Servers/Versions/Users/All Users

2.4.2. Servers Node

Path

ODBC Access/Servers

Overview

When the Servers node is open, it displays a list of servers the Administrator is aware of. These are machines that might house the ODBC Access Windows server, but they are not all servers. The ODBC Access Windows server can also be installed on a Windows XP Service Pack 3, Windows 7 Service Pack 1 (or later) or Windows 8 workstation or later for low volume use, such as that required by a developer.

It is not practical to list all machines on a large network. List only the machines you designate as servers and want the Administrator to work with to appear in the list.

Adding Another Server

To add a server, select the Servers node and then select New from the context menu or select the button. Select a server name from the drop down list or supply a server name. That server is added to the list and reappears each time the Administrator is opened. You can supply a machine name that does not house the ODBC Access Windows server. In that case, the machine is still added to the list, but when that machine's node is expanded, no data is visible under it until the ODBC Access Windows server is installed on it.

Note: *The server name is not verified at this point, but, when you try to connect to it, the connection fails if it is not a valid machine name.*

Removing an Existing Server

To remove a server from the list, select the node for that server and then select the Remove button.

2.4.3. Versions Node

When a specific version is first installed or when Security Configuration is selected from the context menu, the Security Configuration dialog box is displayed.

This dialog box appears only in the Administrator running on the same Windows server as the ODBC Access Windows server. It appears automatically only if security has not already been set for this release. Its purpose is to enable you to set security on the ODBC Access administrative components. Once this has been done, the dialog box can be invoked from the context menu for a specific version to change the way security is configured.

- The default and recommended choice is Configure with Data Access security. This ensures that the ODBC Access administration is secure. Only the Data Access Administrators group and a privileged user account that is used internally by ODBC Access are created. You can change the name of the group or user. If you are on a Windows domain, your account must be a domain administrator in order to select this option. The builtin administrator account, called “Administrator”, is a local account and not a domain administrative account by default. If you are not on a domain, then your account must be a local administrator to select this option.
- The alternative, Configure with default system security, makes use of the security that is already configured on the machine. In most cases, this equates to almost no security. This has an impact on the requirements of Data Access administrator accounts. If Data Access security is selected a Data Access administrator’s account can be an ordinary unprivileged account. When default system security is selected, a Data Access administrator must be a local Windows administrator to perform some functions, such as starting or stopping services, and must be a Windows Domain Administrator to perform remote administration. To select this option, your account must be a local administrator.

When Data Access security is selected, the specified privileged user account might already exist in the Windows domain or on the server. If this happens, the Configure Unisys ODBC Access Information dialog box is displayed.

The following choices are available:

- If the privileged user was created by a previous installation of ODBC Access and the password was not changed, select the first choice. (Prior releases of ODBC Access do not have a security configurator, so this option cannot apply to an upgrade from them.)
- If the user was created by a previous installation of ODBC Access and the password changed or if the user was created independently and conforms to ODBC Access needs, you can select the second option and specify the password for this account. If possible, obtain the password for the privileged user. If the password is unknown, delete the existing ODBC Access privileged user and security. If there are other releases of ODBC Access running that depend on that user, they will fail if the user is deleted. Use the third option if this is not acceptable.
- If the previous options are not appropriate, select the third option to specify a different user name that does not exist in the domain or on the server.

2.4.4. Installations Node

Path

ODBC Access/Servers/Versions/Installations

Overview

This release of ODBC Access does not permit multiple installations of the same release level on one machine. This node always shows only one installation called "Default".

Note: *If more than one installation of a single release level of the ODBC Access Windows server is required, the recommended procedure is to install them on different Windows servers. This configuration is permitted by your license and is easy to administer by means of the Administrator.*

Service Status

Each installation of ODBC Access is represented on its host Windows server by a Windows service. This service accepts connections to the ODBC Access SQL Server. The status of the service is visible in the right-hand pane.

When the service is running, there is a button for Windows to stop it. Stopping the service prevents new connections from being established and terminates any existing connections.

When the service is stopped, there is a button for Windows to start it. This service must be running in order for the ODBC Access SQL Server to function.

Note: *If the Configure with default system security option was selected from the Security Configuration dialog box, it cannot start or stop a service on the local machine unless your account has local administrative privileges, and it cannot start or stop a service on a remote machine in a domain unless your account has domain administrative privileges.*

2.4.5. Databases Node

Path

ODBC Access/Servers/Versions/Installations/Databases

Overview

This node displays a list of the databases configured or managed by the specified installation of the ODBC Access Windows server.

IAConnectTest Database

For each installation of the ODBC Access Windows server, there is one fixed database called IAConnectTest. The database is built into the ODBC Access Storage server in the OS 2200 environment. It is not a real database that exists independently in the Network Database server (or some other storage system), but behaves like a real database because any client can connect to it and retrieve data from it.

The purpose of IAConnectTest is to permit early testing of the configuration without having to learn how to use the ODBC Access Modeller to create a relational view of part of a Network Database server database.

The database definition can be browsed from the Administrator, just like any other database. It consists of one table (test_table) with one column (test_column) and five rows.

The IAConnectTest Database definition is created when the product is installed. When you first add an OS 2200 host in the administrator, the IAConnectTest database automatically becomes associated with that host and can be used to test a connection to it. If you subsequently add another OS 2200 host and want to use the IAConnectTest database to test a connection to it, you must use the OS host node that is subordinate to it in order to associate it with a different host.

Database Status

Each database in the list can also have an auxiliary symbol that indicates its current status. The following status symbols are defined:

A connection to this database is active from this Administrator.

 The previous mapping operation on this database failed.

 The configuration information for this database was lost.

If a database does not have any of these auxiliary symbols displayed, there are no known problems with it and you are not connected to it.

The configuration information is held in the config.ini file in the installation folder of the ODBC Access Windows server. If this file is deleted or overwritten by reinstalling ODBC Access, the configuration information is lost. It can be reconstructed through the Administrator by selecting the OS host node under each database and supplying the correct information.

Connecting to a Database

All activities on a database require an active connection to that database. The Administrator automatically connects and disconnects as required.

When a connection is established for the first time after the ODBC Access Administrator is started, a log-on dialog box is displayed. You need to supply the user name and password at this time. After that initial connection, all information, including the password, is retained until the ODBC Access Administrator is closed. In the interim, connections can be closed and reopened transparently in the background.

Loading the Catalog for a New Database

Before creating and loading the catalog for a new database, the mapped database definition must be created using the ODBC Access Modeller. Its output DDL (DROP_DDL) and MSS files must be present in the DDL folder on the machine that houses the ODBC Access Windows server.

The catalog character set option selects which character set is used to store identifiers in the Database Catalog. If you want to store identifiers, for example, table and column names using Kanji characters, you must select Unicode (UTF-8) from the drop down box. Otherwise, use the Unicode option.

Supply a database name that corresponds to the mapped database name created in the ODBC Access Modeller. Select the OS host name from the list.

Ensure that the OS 2200 host the database resides on is included under the host node for that installation. If it is not, it must be added first. See “OS Hosts” for details.

Select the Databases node and choose New from the context menu. Supply the password for systpe, the super user.

ODBC Access

Select this option if you want to access this database or data source from an ODBC Access driver. This selection cannot be removed when reloading the catalog. In order to remove the selection, you must delete the Administrator records of the database and create it again. If ODBC Access is not currently selected, it can be added when reloading the database definition later.

Open All Areas

Open All Areas specifies whether all database areas are opened when a database connection is established. This is not commonly required.

Depart After Commit

If Depart After Commit is selected, then ODBC Access fully disconnects from the database each time a commit is done. By default, ODBC submits a commit after each statement. This behavior adds minimal overhead while increasing the concurrency with limited UDS slots. Selecting this option is recommended.

Reload/Apply External Script Status Dialog Box

The next dialog box indicates which actions are performed. The most commonly required actions are preselected.

You must run an external script to change permissions or create standard views. For example, Apply External Script must be selected and the script location specified in the Select External Scriptfield. This procedure takes place on the Windows server, which houses the ODBC Access Windows server. If the script is not on this machine or if you are running the Administrator from a remote machine, the best way to avoid confusion about the location of this script is to use a UNCname (for example, \\Machine\share\folder\...\script).

The script specified here is not an ISQL script. This script contains only the SQL commands that must be executed. It cannot have connect or disconnect statements or anything, such as SET, that alters the ISQL state.

After choosing OK, an empty catalog is created and the table definitions are loaded and optionally, an external script is run. While this is taking place, status information is displayed in the status bar of the main Administrator window. As each step completes, a check mark is placed next to it in the preceding dialog box.

If an error occurs while creating the relational catalog, the whole operation fails and the database is not available until the problem is corrected. In this case, the database is marked with ✕ in the Administrator.

Updating a Database Definition

Select the OS host node for the database and review the host name and other options in the right-hand pane. Make changes if necessary.

You cannot remove the SQL Access (ODBC) selection.

Select the node for the database that must be reloaded and select Reload Database/Apply Script.

The next dialog box indicates which actions are performed. The most commonly required actions are preselected.

You must run an external script to change permissions or create standard views. For example, Apply External Script must be selected and the script location specified in the Select External Script field.

After choosing OK, an empty catalog is created and the table definitions are loaded and optionally, an external script is run. While this is taking place, status information is displayed in the status bar of the main Administrator window and as each step completes, a check mark is placed next to it in the preceding dialog.

Removing a Database

Note: *This procedure does not remove a Network Database server database. It only removes this particular ODBC Access definition of it.*

Select the database node that must be removed, then select Remove from the context menu.

2.4.6. OS Host Node

Path

ODBC Access/Servers/Versions/Installations/Databases/OS Host

Overview

The host node shows information about the host on which this database resides.

The following information is important:

- TCP/IP Address/Host Name: The ODBC Access Windows server uses this name or address to connect to this machine. This field cannot be changed. If the database is moved to another OS 2200 host, then the database definition must be mapped again on the new machine.
- TCP/IP Service/Port Name: The ODBC Access server in the OS 2200 environment is configured on this service name or port number. This is tied to the host and cannot be changed here. See the "OS Hosts" topic for instructions on how to change it.
- Whether the database can be accessed through the ODBC Access SQL Server. Removing this entry is not permitted.
- Whether all database areas must be opened whenever a connection with the database is established.
- Whether ODBC Access should disconnect from the database every time a commit (or rollback) statement is submitted. This provides for greater throughput with few UDS slots.

2.4.7. Tables Node

Path

ODBC Access/Servers/Versions/Installations/Databases/Tables

Overview

The Tables node lists all the tables that have been defined for the database. Select a specific table for information about that table. Each table entry displays the following information about the table:

- The name of the owner of the table.
- The name of the creator of the table.

- The percentage of free space (% Free Space) in the table. This is always set to 20. It exists only to satisfy an SQL catalog requirement. It has no meaning within the context of the Network Database server databases.
- The type from the relational catalog. It should always be "T" for table.
- Presence or absence of any primary key constraints.
- Presence or absence of any foreign key constraints.
- Presence or absence of any check constraints.
- Presence or absence of any user constraints.
- The storage system for the table. For most user tables, the storage system is the OS 2200 Storage system. System tables are in the Windows storage system.

Table permissions are set at the Users node for the selected table. For information on how to do this, see the “Users Node” topic.

Adding a Table

Because ODBC Access only reflects the state of a Network Database server database, it is not possible to add a table through ODBC Access. In order to add a Network Database server table, follow the instructions for adding records to a Network Database server database and then remap the database and reload the ODBC Access catalog for that database.

Changing the Name of a Table

The initial table names are automatically derived from the Network Database server names. You can change the name of a table using the ODBC Access Modeller. For more information on the Modeller, refer to the *ODBC Access Modeller User’s Guide.*

2.4.8. Columns Node

Path

ODBC Access/Servers/Versions/Installations/Databases/Tables/Columns

Overview

The Columns node lists all the columns in a table. Select a specific column for full details on that column.

Each column entry displays the following information about the column:

- Name of the owner of the column
- SQL data type
- Default value for the column
- Width
- Scale
- Character set for the data of that column data
- Collation

Adding a Column

ODBC Access only reflects the state of a Network Database server database. You cannot add a column through ODBC Access. In order to add a column, you must add the corresponding field in the underlying database and then remap and reload the ODBC Access catalog for that database.

Changing the Name of a Column

The initial column names are automatically derived from the Network Database server field names. You can change the name of a column using the Modeller. For more information on the Modeller, refer to the *ODBC Access Modeller User's Guide*.

2.4.9. Indices Node

Path

ODBC Access/Servers/Versions/Installations/Databases/Tables/Indices

Overview

The Indices node lists all the indices defined for the selected table. Each index entry also shows the columns that participate in the index and, for each column, whether the index is ascending or descending, and its component number if it is part of a multicomponent index.

There are no operations that can be performed on indices by the Administrator.

2.4.10. Tables/Users Node

Paths

ODBC Access/Servers/Versions/Installations/Databases/Tables/Users

Overview

Each table has a subordinate node that shows the users authorized to access that table. Selecting a specific user shows that user's current access permissions for that table. It also shows whether the user is a DBA or has RESOURCE rights.

You can grant a right to a special user called "Public". When rights are granted to Public, every user has those rights and they are shown under the Users node. Also, another approach is to show Public as a user name and only the other users with explicit rights to a table are shown under the Users node.

For example, if SELECT, INSERT, UPDATE, and DELETE rights are granted to Public for a table and no other rights are granted, then the only entry under the Users node is the user Public. Everyone then has SELECT, INSERT, UPDATE, and DELETE privileges for that table.

Unexpected Behavior

Access permissions are governed by the standard SQL behavior of the GRANT and REVOKE statements. The implications of this are not always intuitive:

- If user Jim has SELECT privileges and Public has SELECT privileges, you cannot remove SELECT from Jim without first removing SELECT from Public.
- If user Fred grants SELECT privileges to Jim and user Carol grants SELECT privileges to Jim, then Fred can revoke Jim's SELECT privileges, but he still has SELECT access, because it was also granted by Carol. When Fred revokes Jim's SELECT privilege, he only revokes the privileges he granted, not those granted by other users.

Granting Access to a New User

Note: *A new user must already be recorded in the ODBC Access SysUsers file. You can verify the presence of the user by referring to the Users node under the Versions node. If necessary, the user can also be added there.*

- Select the Users node and then choose New from the context menu. A list of all current users of this version or release level of ODBC Access is displayed.
- Select the user you want to add.
- Set access permissions.
- Choose the Update button on the tool bar to complete the changes.

Changing User Access Rights

- Select the user whose rights you wish to change. The access rights are displayed in the right-hand pane.
- Each access right or privilege is marked with a "Yes" or a "No". Choose the access right to toggle the privilege to its opposite state.
- Set the appropriate radio buttons to grant the user the DBA, RESOURCE, or no privilege.
- Choose the Update button on the tool bar to complete the changes.

Note: *Some access rights might be marked with an asterisk. These represent privileges that you cannot change, either because you did not grant them or because you do not have the DBA privilege.*

Removing User Access

- Select the user whose rights you want to remove. The access rights are displayed in the right-hand pane.
- Set all the permissions to No.
- Choose the Update button on the tool bar to complete the changes.

2.4.11. Views Node

Path

ODBC Access/Servers/Versions/Installations/Databases/Views

Overview

The Views node lists all the views defined for the database. View definitions can be created using the interactive View Builder that forms part of the Administrator, or they can be created from other sources, such as ISQL or ODBC, etc. Views that are created from other sources occur in the relational catalog and can be viewed here. They cannot be modified. If you need to change one of these views, they must be removed and recreated.

Views that are created using the interactive View Builder maintain a record of the view structure that is independent of the relational catalog, as well as the record of the view within the relational catalog. These views can be modified using the interactive View Builder.

When a database is remapped, all the view definitions in the relational catalog are lost because the catalog is recreated as part of the relational mapping process. Definitions of views created with the interactive View Builder are retained in their own separate storage area and can easily be added back into the catalog from there.

Each view in the list visible under this node is signified by one of three symbols:

Indicates that the view was created by the interactive View Builder and also exists in the relational catalog. It can be modified using the View Builder.

Indicates that the view was created from another source. It exists in the relational catalog, but cannot be modified.

Indicates that the view was created by the View Builder, but is not in the relational catalog. The ODBC Access SQL Server is not aware of the existence of this view, but it can be replayed to put it back in the catalog.

Select a specific view for information about that view. Each view entry displays columns included in the view and its SELECT clause. This information is not available for view definitions that are not recorded in the relational catalog.

Each view that is recorded in the relational catalog also has a subordinate node, which shows all the users who have access to the view and their access rights. Access rights for views are set in exactly the same way as for tables.

Note: *When tables are removed or changed in any way, views that depend on them are not modified or dropped. It is up to you to remove or redefine views that have invalid dependencies. When a view is opened using the interactive View Builder, its definition is validated and any invalid dependencies are clearly marked for removal or modification.*

Creating a New View

The Administrator includes an interactive View Builder. Invoke the View Builder to create a new view as follows:

- Select the Views node, then select New from the context menu.
- If necessary, review the detailed instructions on the View Builder.

Changing a View

A view can be modified only if it was originally created by the View Builder. These views are signified by the or icons.

- Select the view you want to change.
- Choose Modify from the context menu.

  This invokes the interactive View Builder with that view loaded.

Instructions on the View Builder can be found later in this section.

Re-creating a View

When a database is remapped, all views are dropped from the relational catalog. View definitions that were created using the interactive View Builder are retained in its own storage area. These views can be replayed to put them back in the relational catalog.

To replay a single view, select the view (designated by the icon) and select Replay View from the context menu.

To replay all views for the database, select the Views node and select Replay View from the context menu.

Removing a View

- Select the view you want to remove.
- Choose Delete from the context menu to remove the view.

View Users

Setting permissions for views is exactly the same as for tables. See the "Tables/Users Node" topic for a description.

2.4.12. Synonyms Node

Path

ODBC Access/Servers/Versions/Installations/Databases/Synonyms

Overview

The Synonyms node lists all the synonyms defined for the database. You can select an individual synonym to view its creation information, the table it is a synonym for, and whether it is public or private.

Creating a Synonym

- Select the table or view node for which you want to create a synonym.
- Select Create Synonym from the context menu.
- Complete the resulting dialog box.

Removing a Synonym

- Select the synonym you wish to remove.
- Choose the Delete from the context menu to remove the synonym.

2.4.13. OS Hosts

Path

ODBC Access/Servers/Versions/Installations/OS Hosts

Overview

A single installation of the ODBC Access Windows server is able to connect to databases on more than one OS 2200 host system. Before doing so, the hosts must be defined here.

When first creating a mapping for a database, you specify one of the hosts in this list to indicate the location of the database. A host node must be created here before any databases can be mapped for that host.

Adding Another Host

To add a new host, select the OS host node, then select New from the context menu. Supply the following information:

- The Host Name. This can be any name you want to use when referring to the host. Its only function is to identify the machine to you.
- The TCP/IP Address/Host Name. This must be the TCP/IP host name as it is recorded in your Domain Name Server (DNS) or name of the host file of the machine on which the ODBC Access Windows server is installed. If you do not have DNS and are not able to update your host file, you can enter the TCP/IP address of the machine instead. This is the address of the TSAM process, which was configured for ODBC Access.

  Note: *It is important to specify the host name or address of the high-speed connection to the OS 2200 host environment for best performance.*

- The TCP/IP Service/Port Name. This field contains the default ODBC Access service, and, it is unlikely that you need to change it. The service does not have to be unique for each OS 2200 host. You must change it only if there is a conflict between ODBC Access and another application. In that case, you must change the service in the environment file in the OS 2200 environment. For more details, refer to the *ODBC Access Installation and Operations Guide*.

Changing Host Parameters

Follow this procedure to change the TCP/IP host name or the TCP/IP service name.

- Select the host node you want to change.
- In the right-hand pane, change the TCP/IP host name or service name.

Removing a Host

Removing a host does not change any configuration in the OS 2200 environment. It only removes the Administrator's knowledge of that host. You cannot remove a host node until all ODBC Access mappings for databases that reside on that node have either been removed or switched to another host.

To remove the host node

- Select the host node you want to remove.
- Choose Remove from the context menu.

2.4.14. Configuration Node

Path

ODBC Access/Servers/Versions/Installations/Configuration

Overview

The Configuration node enables general client and server configuration information for the installation to be set. The node has two tabs: one for client configuration and one for server configuration.

This node is not used frequently because the client configuration applies only to the use of ISQL on the same machine as the ODBC Access SQL Server and the server configuration tab contains rarely changed configuration and trace parameters.

Client Service

This is the TCP/IP service name (as resolved on the server) or the port number on which ISQL running on that server uses to connect to the ODBC Access SQL Server.

Note: *The Client Service does not apply to ODBC clients, and it does not apply to ISQL running on other machines.*

Select Character Set

This is the character set used by ISQL running on the same server as the ODBC Access SQL Server.

Note: *It does not apply to ODBC clients, and it does not apply to ISQL running on other machines.*

TCP/IP Address/Host Name

This is the TCP/IP host name (as resolved on the Windows server, not a remote Administrator machine) of the default OS 2200 environment to which ODBC Access connects. The TCP/IP address can be entered if desired. It is necessary to maintain this value only if technical support requires you to perform manual mapping operations. If the Administrator is used for all mapping operations, then each database records the host it is associated with and the default is not necessary.

TCP/IP Service/Port Name

This is the TCP/IP service name (as resolved on the Windows server, not the remote Administrator machine) of the default port on which the ODBC Access OS 2200 components on the default host are configured. The port name can also be entered. It is necessary to maintain this value only if technical support requires you to perform manual mapping operations. If the Administrator is used for all mapping operations, then each database records the host it is associated with and the default is not necessary.

Product Key

This is the product key for the ODBC Access SQL Server installation. Whenever a new product key is received, it is entered here. The product key is only validated and loaded by the server the next time someone connects to the ODBC Access SQL Server.

Server Service

This is the TCP/IP service name or port on which the ODBC Access SQL Server listens for client connections. It is not likely you need to change this value. If it is changed, then all clients must be changed to match this value.

Log Level

The log level is used for low-level tracing and should be set only with specific instructions from technical support.

Tracing is normally set for a specific user from the All Users node.

RPC (Remote Procedure Call) Debug

The RPC debug field is used for low-level tracing and should be set only with specific instructions from technical support.

Tracing is normally set for a specific user from the All Users node.

Access Mode

This parameter sets the access mode for the entire ODBC Access Windows server. It applies to all defined databases.

- Read Only causes all Network Database areas to be opened in read-only mode and updates are not possible.
- Request Update causes sessions to be read only by default, but an ODBC Access driver can specifically request an update session by placing a ".u" at the end of the database name. Default Update permits sessions to update the database. An ODBC Access driver can specifically request a read only session by placing a ".r" at the end of the database name.

2.4.15. Users Node

Path

ODBC Access/Servers/Versions/Users

Overview

The Users node shows all the users associated with a particular release level or version of ODBC Access. These users appear under the All Users subordinate node. The node also shows all the users currently connected to ODBC Access under the Active Users subordinate node.

User information is held in a Distributed COM (DCOM) component called Unisys Data Access SysUsers, where it is shared by the ODBC Access SQL Server, and one or more copies of the Administrator. When it is run as a service (default), then it stays active all the time. If it is not in use by either of these components, it automatically saves its contents to a backup file called SysUsers in the bin folder within ODBC Access Windows server's installation folder and then unloads itself from memory. The next time it is needed, it starts up automatically.

ODBC Access offers several forms of authentication and these can be set at the user level. For example, some users might have Data Access authentication, others might have Windows domain authentication. Full details on security and authentication can be found in the *ODBC Access Installation and Operations Guide*.

These are the available options:

- Data Access. Authentication takes place on the ODBC Access user database in the Windows environment. Passwords are encrypted, and there is a simple lock-out mechanism. It is suitable for people who do not have a Windows domain account.
- Windows domain. Authentication takes place using the Windows security system. By default, the primary domain of the Windows server that houses the ODBC Access Windows server is used, but this can be changed if desired.
- Preauthorized. This should be used only in secure networks where you do not require additional authentication from ODBC Access. An example of this would be a network where everyone is identified by means of a smart card, by fingerprints or, by some other biometric authentication method. In all other cases, this equates to no authentication.

2.4.16. All Users Node

Path

ODBC Access/Servers/Versions/Users/All Users

Overview

This node lists all the users for a version or release level of ODBC Access. When the ODBC Access Windows server is installed, a SysUsers file is installed, which contains two accounts:

- A default user account (default_user) is marked with . This account contains the default parameters, which are used to create new user accounts. Any user can be designated as the default user, but there can only be one.
- The ODBC Access super user account (systpe). This account owns all system tables and automatically has all privileges. It is set up to use Data Access security.

Adding a New User

Follow this procedure to add a new user.

Note: *Unless the default user account is set to Data Access authentication, it is not necessary to add new user accounts. They are added the first time they are used. This is permissible because all other authentication methods take place outside of the ODBC Access environment, so user accounts here are used only for tracking purposes.*

- Select the All Users node.
- Select New from the context menu.
- Complete the New User dialog.

Because adding a new user is not a common operation and the information supplied here is the same as when a change is made, the information required for this dialog is described in the Changing a User section.

The only exception is the Name field, which is supplied here and which cannot be changed.

Name

The name is the user name or usercode that is used to connect to the system and identifies the user when they have connected. It is a required field. The requirements for name vary according to the authentication method used.

When Data Access authentication is used, the name can be up to 100 characters in length and can contain any lowercase characters and any special characters, including spaces.

Note: *If spaces are included in Name, then some products might require that the name be enclosed in quotation marks when entered.*

When Windows domain authentication is used, the name must be a legitimate Windows domain user name.

Note: *The name must always be specified in lowercase here.*

Changing a User

A user's information can be changed by selecting the Users node, then altering the information presented in the right-hand pane. The user name cannot be changed and, depending on the authentication method, other fields might be disabled.

Password

The password is relevant only when the authentication method is Data Access.

When the authentication method is Data Access, the password can be up to 100 characters in length and can include any characters (including spaces) except a comma (,). The password must be at least one-character long. If the field appears blank, it contains one or more spaces. A password that consists only of spaces is acceptable, but it is confusing, so it is not recommended.

Note: *If spaces are included in Password, then some products might require that the password be enclosed in quotation marks when entered.*

Max Bad Logons

Max Bad Logons is the maximum number of bad connection attempts allowed for this user before the user account becomes disabled. A bad connection attempt occurs when a legitimate user name is supplied with an incorrect password. Once the account has been disabled, the user is not permitted to log on, even if they supply a correct password, until an administrator has enabled the account.

Note: *Max Bad Logons is applicable only to Data Access authentication. A zero in this field indicates that Max Bad Logons is not set for this user.*

Disabled

If the number of bad connection attempts equals or exceeds the Max Bad Logons value, the account is disabled and Disabled is selected. The user's account can be enabled again by removing the selection. The number of bad logon attempts is increased automatically only when Data Access authentication is selected; therefore, this feature applies only to that authentication method.

A user account can also be manually disabled (irrespective of the value of Max Bad Logons and the number of bad connection attempts) by selecting Disabled. A user account can be disabled regardless of which authentication method is selected. This state is checked only when a user attempts to connect to the system. It has no effect on a user who is already connected. To terminate an active user's query, select the user's name under Active Users, then select the Kill Query button on the Dynamic tab.

Security Type

Four choices are presented in this list. Windows authentication has two suboptions. A description of the Security Types can be found later in this section and also in the ODBC *Access Installation and Operations Guide*. This is a list of available security types:

- Data Access Security
- Windows Security (Impersonate)
- Windows Security (Do Not Impersonate)
- Preauthorized

Limits I/O

A positive value indicates the maximum number of ODBC Access I/Os allowed for any query initiated by this user. An ODBC Access I/O, in this context, is a network request between the ODBC Access SQL Server and the storage system, which houses the database. An error is returned to the user if this limit is exceeded. A zero in this field indicates that the I/O limit is not set for this user.

Limits Seconds

A positive value indicates the elapsed time, in seconds, permitted for any query initiated by this user. This is elapsed wall-clock time. An error is returned to the user if this limit is exceeded. A zero in this field indicates that the seconds limit is not set for this user.

Limits Rows

A positive value indicates the maximum number of rows that can be returned by a query initiated by this user. The number of rows returned is not necessarily an indication of the amount of work required to complete a statement. For example, a query might need to scan 100,000 rows in two tables in order to return a result set that is 10 rows long. An error is returned to the user if the limit is exceeded.

Removing a User

To remove a user

- Select the Users node.
- Choose Remove from the context menu.

Setting the Default User

To make a user the default user

- Select the Users node.
- Choose Make user default from the context menu.

There is always only one default user. The default user supplies information to all newly created user accounts, whether these are created manually through the ODBC Access Administrator or automatically by the ODBC Access Windows server. The ODBC Access Windows server can create user account records automatically when the authentication method for the default user is not set to Data Access authentication.

2.5. Security Types

This section describes the authentication choices as they appear in the Security Type field of the New User dialog box and the Static tab. For more information on authentication methods, refer to the *ODBC Access Installation and Operations Guide*.

These choices differ from what is described in the *ODBC Access Installation and Operations Guide* in that some of the authentication methods have been subdivided here for clarity.

For each authentication method, one or more of the following requirements are listed:

- A Windows account for each user
- A manual entry in the ODBC Access user database for each user

The following tables assist you in choosing appropriate authentication methods. You can select more than one. These parameters can be set at the user level, so, for example, some users might use Data Access authentication and others might use Windows.

This table shows the possible and recommended authentication methods depending on the type of accounts a user has.

User has...	Possibilities	Recommendations
Smart cards, etc.	All	Preauthorized
Windows account	Preauthorized Data Access Windows	Windows
No Windows account	Data Access Preauthorized	Data Access

The next table lists the amount of administrative overhead associated with each authentication method.

Authentication Method	Administrative Overhead
Data Access	High
Windows	Medium
Preauthorized	Low

If you set Windows authentication for users who do not have Windows accounts, the administrative overhead in that environment increases.

2.5.1. Data Access Security

Requirements

- Data Access

Description

When Data Access Security is selected, authentication takes place on the ODBC Access user database. The Data Access rules for user names and passwords apply.

The ODBC Access user database is maintained in the Windows environment where network file system (NFS) security might be used to restrict access to it and where all sensitive information, such as passwords, is encrypted.

This method offers a simple lock-out mechanism. A maximum number of bad logon attempts can be set. When a user has attempted to connect that number of consecutive times with a bad password, the account is disabled. When the account has been disabled, the user cannot connect even if they supply a correct password, until the account has been enabled again by an administrator.

2.5.2. Windows (Impersonate)

Requirements

- Windows

Description

When Windows (Impersonate) security type is selected as the default, the user must have a Windows domain account. It is not necessary to make a manual entry in the ODBC Access user database, one is added automatically.

Note: *Do not use this method unless you are familiar with Windows security and are able to set appropriate permissions for all ODBC Access users. The permissions govern users access to all ODBC Access resources in the Windows environment.*

All the rules regarding Windows domain user names, passwords, and lock-out mechanisms are enforced. A Windows domain controller must be available to permit connection to ODBC Access.

A user's connection request is accepted or rejected at the time they attempt a connection to ODBC Access.

A password is not required in the ODBC Access user database, and, if one is supplied, it is ignored.

A key feature of this method is that the ODBC Access session in the Windows environment runs within the security context of the connected user (that is, the user is impersonated). Each ODBC Access user must have permission for each ODBC Access resource in the Windows environment.

When this method is selected, the Advanced button becomes available. This controls how the Windows domain authentication takes place. Even in a multidomain environment, it is not necessary to make any changes to the default value, but a description of the resulting dialog box can be found in Windows Advanced Options later in this section.

2.5.3. Windows (Do Not Impersonate)

Requirements

- Windows

Description

When the Windows (Do Not Impersonate) security type is selected as the default, the user must have a Windows domain account. It is not necessary to make a manual entry in the ODBC Access user database; one is added automatically.

Note: *Of the two Windows authentication options, this one is recommended for most sites.*

All the rules regarding Windows domain user names, passwords, and lock-out mechanisms are enforced. A Windows domain controller must be available to permit connection to ODBC Access.

A user's connection request is accepted or rejected at the time they attempt a connection to ODBC Access.

A password is not required in the ODBC Access user database, and, if one is supplied, it is ignored.

A key feature of this method is that the ODBC Access session in the Windows environment runs within the security context of the Data Access TCP service, which is normally the System account. This simplifies the Windows security configuration so that it is unlikely that any specific changes are required for ODBC Access.

When this method is selected, the Advanced button becomes available. This controls how the Windows domain authentication takes place. Even in a multidomain environment, it is not necessary to make any changes to the default value, but a description of the resulting dialog box can be found in Windows Advanced Options later in this section.

2.5.4. Windows Advanced Options

This topic describes the advanced options available when Windows domain authentication is chosen. It describes the options available for designating the domain that performs the authentication and the order in which domains are searched.

When the Advanced button is selected, the *Windows Security* dialog box is displayed

Note: *Although this dialog box is accessible from each user's information, it is used to set parameters that are global to all users with the Windows authentication method.*

In addition to choosing OK on this dialog box, you must choose Update on the user's Static tab in order to commit these changes.

Domain of Server

This is the default.

The domain of the machine on which the ODBC Access Windows server is installed is used as the authenticating domain.

Server's Local Account

Authentication takes place only on the database of the local account of the machine on which the ODBC Access Windows server is installed. No domain accounts are consulted. This method might be used if ODBC Access is installed on a Windows server that does not participate in a Windows domain.

Server's Local Accounts then Trusted Domains

The local accounts database on the Windows server is searched first. If the user name is not found there, all trusted domains are searched. If the user has a local account on the machine on which the ODBC Access Windows server is installed, it is used even if the user also has a domain account.

This Domain

Authentication must take place using the specified domain only.

2.5.5. Preauthorized

Description

When the Preauthorized security type is selected as the default, new users do not need a Windows domain account. It is also not necessary for the Administrator to make a manual entry in the ODBC Access user database; one is added automatically.

Note: *This method is recommended only on a secure network because it essentially equates to no authentication on the part of ODBC Access. However, beyond authentication, the normal SQL controls on tables still apply.*

No authentication takes place. It assumes this was already done when the user connected to the network.

A user's connection request is always accepted.

A password is not required in the ODBC Access user database, and, if one is supplied, it is ignored.

2.5.6. Active Users Node

Path

ODBC Access/Servers/Versions/Users/Active Users

Overview

This node shows all users who are currently connected to the ODBC Access Windows server. The name shown is the user name with which they connected.

If the same user name connects more than once, then each connection is shown separately in the list with a unique number in parentheses next to it. This number corresponds to the process ID on the Windows server and can be used in conjunction with the Windows Task Manager or a process viewer to identify the session on the Windows system.

Selecting a specific user displays the dynamic user information in the right-hand pane. This information refreshes automatically.

2.5.7. Dynamic Tab

The Dynamic tab is displayed when an active user is selected.

The Dynamic tab shows a user's resource usage as a percentage of their specified limits. The user's currently executing query can also be terminated from this tab.

Kill

The Administrator can kill an active user's query. In most cases, the query terminates immediately, the user receives an appropriate error message, and the user can then continue with work. In cases when a push-down predicate is being processed, there might be a long delay before the query is terminated. A push-down predicate is used when nonindexed fields of the table must be scanned. This involves filtering in the Storage Server environment. While this is taking place, there is no activity in the ODBC Access Windows server. As soon as activity is resumed in the ODBC Access Windows server, the query terminates.

Limits

The Limits progress bars indicate the current resource usage for the user for the query that is currently executing. It is expressed as a percentage of the specified limit. If no limit is set for a category (I/O, Seconds, or Rows), then the corresponding bar is disabled.

2.6. View Builder

This topic describes the steps necessary to create a view using the Administrator's View Builder.

Because ODBC Access incorporates a relational database system, you can create views in the same way as any other relational database using the CREATE VIEW statement. The Administrator's View Builder provides a graphical alternative. It permits the creation of views by selecting and combining components. You can create advanced views incorporating scalar functions and arithmetic and literal expressions with this tool.

The steps required to create a view using the View Builder are as follows:

- Choose a name for the view.
- Select the table or tables on which the view is based.
- If it is a simple view, select the columns to include in the view.
- If it is a complex view, which incorporates expressions, create the expressions first and then select the columns and expressions to include in the view.
- Create conditional expressions for the WHERE clause.
- Select the conditional expressions for inclusion in the WHERE clause.

If a view is created with the View Builder, it can also be modified by it. This is possible because the definitions of views created with the View Builder are stored in the View Builder's own storage area, as well as in the ODBC Access SQL Server's relational catalog. If a view is created by other means (for example, ISQL), then the View Builder does not know its definition. Although the Administrator shows its presence and displays minimal information about it, the View Builder cannot change its definition. Views in the relational catalog not created by the View Builder are designated by the icon.

When a view created by the View Builder is modified, it is possible that the underlying table information might have changed. For example, a table or column that the view depends on might no longer exist. Normally, this is reported as an error when you attempt to use the view. However, the View Builder performs a consistency check when it is invoked. You might choose to automatically discard all components of the view that depend on items that no longer exist, or you might choose to take responsibility for correcting the errors yourself. If the latter option is chosen, all view inconsistencies are shown in red text with the strike-through attribute (for example, ~~customer.history~~).

2.6.1. View Name

Type a name for the view in the View Name field. The name must be a valid SQL identifier.

2.6.2. Select Tables

The select tables tab shows a list of all the tables in the database in the left column. To include a table in the view, select the desired table from the Select Tables list, then choose the **>>** button to move it to the Selected Tables list.

If you change your mind and want to remove a selected table, select that table name and use the **<<** button to remove it from the Selected Tables list. This operation is not available after a tab other than Select Tables has become active.

Note: *ODBC Access does not allow more than five tables to participate in a join. Including more than one table in a view implicitly joins the tables. Performance is normally enhanced if you minimize the number of joins and the number of tables included in a join. The most important criterion, though, is the composition of the WHERE clause. For best performance, include keys and ensure there are no conditions linked with an "or", which prevents the keys from being used.*

The "dharma ORDERED" option can be applied to the first table in the list to indicate that normal optimization must be overridden and the tables are joined in the order they are listed. This option should be used rarely and with caution. Refer to the *ODBC Access SQL Reference Manual* for details on the dharma ORDERED clause.

2.6.3. Select Column or Expression

This tab shows a list of all the columns or expressions for the selected tables in the Available Column or Expression list. This list also shows all literal constants and all column expressions that have been defined on the Setup Column Expression tab. If you require an expression and it does not appear in the Available Column or Expression list, select the Setup Column Expression tab to define it (See “Setup Column Expression”).

To include a column, literal value, or expression in the view, select the desired item in the Available Column or Expression list, then choose the **>>** button to move it to the Selected Columns list. The Column Heading name is automatically derived from the selected column. The name can be changed by double-clicking the Column Heading name.

If you want to include a literal value that is not already in the Available Column or Expression list, enter it in the Enter Literal field and choose the **>>** button to move it to the Selected Columns list. It is added to the list so that it can be used in other contexts.

If the literal value is numeric, enter the number. If it is a character value, you can either enclose it in single quotation mark characters (') or select the Alpha check box. The single quotation mark characters are added for you. Do not do both.

Choose OK to create your view.

2.6.4. Setup Column Expression

This tab is required only for complex views that require column expressions such as one of the following:

```
select name, base_salary, sales * commission from...

select upper (city), to_char (sysdate (), 'yyyy/mm/dd'), month (sysdate ())
from...
```

In each of these cases, arithmetic expressions or scalar functions and literal values need to be supplied. Use this tab to define the required expressions (including the scalar functions) and then return to the Select Column or Expression tab to include them in the view.

Building an Expression Based on a Function

- Select an item from Available Column or Expression.
- Right-click to obtain the context menu.
- Select the desired class of function.
- Select the desired function (not all functions are available in this release).
- Complete the resulting dialog box.
- That expression then appears in the Available Column or Expression and can be used as a component in a more complex expression.

For example, if you select the Substring function from the context menu for the column "customer.zip", the Substring function dialog box is then displayed. The character expression, char_expression, is simply the customer.zip, column and the start position and length are 1 and 5 respectively.

Once the substring function has been defined, it appears in the Available Column and Expression list. Return to the Select Column or Expression tab and select the function.

Building an Expression Using an Operator

- Select an item from the Available Column or Expression.
- Select the Col/Exp/Lit button to copy it to the Expression field.
- Select the desired operator from the Operators column.
- Select the Op button to copy it to the Expression field.
- Select an item from the Available Column or Expression.
- Select the Col/Exp/Lit button to copy it to the Expression field.

As soon as that sequence is complete, the expression appears in the Available Column or Expression list and can be used as a component in a more complex expression.

The Expression field clears, and can then be used to define another expression.

If you make a mistake during the construction of an expression and want to start over, select the Reset button.

If you want to include a literal value that is not already in the Available Column or Expression list, enter it in the Enter Literal field and select the Col/Exp/Lit button to move it to the expression field.

If the literal value is numeric, enter the number. If it is a character value, you can either enclose it in single quotation mark characters (') or select the Alpha check box. The single quotation mark characters are added for you. Do not do both.

2.6.5. Setup Condition

This tab is used to create conditional expressions that are used in the WHERE clause of the view definition. All previously defined column expressions can be used to form the conditional expression, and complex conditional expressions can be built from simpler components.

- Select an item from the Available Column or Expression.
- Choose the Setup Col button to copy the item to the Condition field.
- Select the desired operator from the Operators column.
- Select the Setup Cond button to copy the operator to the Condition field.
- Select another item from the Available Column or Expression list.
- Select the Setup Col button to copy the item to the Condition field.
- As soon as that sequence is complete, the expression appears in the Available Column or Expression list and can be used as a component in a more complex expression.

The Condition field clears and can then be used to define another expression.

If you make a mistake during the construction of an expression and want to start over, choose the Reset button.

If you want to include a literal value that is not already in the available columns area, enter it in the Enter Literal field and select the Setup Col button to move it to the Condition field.

If the literal value is numeric, enter the number. If it is a character value, you can enclose it in single quotation mark characters (') or select the Alpha check box. The single quotation mark characters are added for you. Do not do both.

2.6.6. Select Conditions

- Select the condition from the Available Condition column.
- Select the **>>** button to copy it to the Selected Condition list.
- If you make a mistake, you can return the condition to the Available Condition list with the **<<** button.
- Select an item from the Available Column or Expression.
- Choose OK to complete the view definition.

To review the final text form of the CREATE VIEW statement generated from the View Builder, choose the OK button.

Choose OK again to create the view.

Section 3
Common Procedures

3.1. Overview

This section describes how to accomplish some common tasks with the Administrator.

3.1.1. Configuration Procedures

- Add a new Windows server
- Add a new OS 2200 host
- Replace lost configuration information

3.1.2. Database Procedures

- Load the catalog for a new database
- Reload Database/Apply external script
- View table definitions
- Create a new view
- Modify a view definition
- Re-create a view
- Create a new synonym
- Change access permissions

3.1.3. User Procedures

- Add a new user
- Make a user the default user
- Set the system's default authentication method
- Set default query limits
- Monitor an active user
- Stop a runaway query

3.2. Configuration Procedures

This topic describes procedures related to the configuration of the system.

3.2.1. Add a New Windows Server

Several copies of the ODBC Access Windows Server can be installed on different servers at a site. The ODBC Access Administrator can administer all of these, but in order to do so, additional Windows servers must be added to the Administrator's list of servers:

- Select the Servers node.
- Select New from the context sensitive menu or select the button.
- Specify the Windows name (not the TCP/IP host name) of the Windows server on which the ODBC Access Windows Server is installed or choose the server name from the drop down list box.

Note: *The server name is not verified at this point, but when you try to connect to it, the connection fails if it is not a valid machine name.*

See “Servers Node” in Section 2, “User Interface,” for more information.

3.2.2. Add a New OS 2200 Host

Before a database can be mapped by the Administrator, details concerning the OS 2200 host environment on which it resides are recorded in the Administrator. Each database is associated with one host, but a single installation of the ODBC Access Windows server can access databases on different hosts.

- Select the OS host node.
- Select New from the context sensitive menu.
- The host node name is any name you choose for the host machine. It does not have to match any other configured name.
- If a TCP/IP host name is supplied, it is the host name as it is resolved on the selected Windows server. If DNS is used or a TCP/IP address is supplied, there is no ambiguity.
- If a TCP/IP service is supplied, it is the service as it is resolved on the selected Windows server. This is almost always iarpc81. A port number might be specified instead. This corresponds to the port number specified in the environment file in the OS 2200 environment. Refer to the *ODBC Access Installation and Operations Guide* and “OS Hosts” in Section 2, “User Interface,” in this guide for additional information.

3.2.3. Replace Lost Configuration Information

If the config.ini file for the specified ODBC Access Windows Server installation is deleted or replaced (for example, when reinstalling the software), the configuration information for each database is lost. This situation is identified by the presence of ? next to each database.

The ideal method of recovery is to restore the config.ini file from a backup version. If this is not possible, the information can be re-entered as follows:

- Select the OS host node under each database marked with .
- Enter the information for that database in the right-hand pane and choose Update.
- Review the Configuration node for the installation. It might need changes, but the defaults are probably sufficient.

3.3. Database Procedures

This section describes procedures related to loading the relational catalog for a database, modifying that definition, and reviewing it.

3.3.1. Load the Catalog for a New Database

This procedure is used to load a database catalog for the first time.

1. If the OS 2200 environment does not have a host node, select the OS Host node to add one to the environment. See “Add a New OS 2200 Host” for more information.
2. Select the Databases node.
3. Select New from the context menu.
4. Specify the password for the user systpe.
5. Specify the mapped database name that was defined in the ODBC Access Modeller.
6. Choose OK. This brings up the progress dialog box. It allows you to monitor the progress of the catalog loading procedure. Status information is also visible in the status bar of the Administrator's main window. You can also specify an external script, which is applied after the catalog is loaded.

3.3.2. Reload Database/Apply External Script

This procedure is used when a change is made to the definition of a Network Database Server database. This procedure assumes you already remapped the database using the ODBC Access Modeller and you have regenerated the output files into the DDL folder in the installation folder of the ODBC Access Windows server.

- Select the affected database node.
- Select Reload Database or Apply External Script from the context menu.
- Supply the password for the user systpe.
- Choose OK. This brings up the progress dialog box. It allows you to monitor the progress of the catalog loading procedure. Status information is also visible in the status bar of the ODBC Access Administrator's main window. You can also specify an external script, which is applied after the catalog is loaded.

You can run an external script to restore view definitions or table and column level permissions.

This method is used to run an external script only. Make sure that the Apply External Script activity is selected only in the Reload or Apply External Script Status dialog box.

3.3.3. View Table or Definitions

This procedure determines what the relational tables for a mapped database look like. The same approach can be used to review view and synonym definitions.

- Select the desired database node.
- Supply any requested connection information (For example, user name, password, chargecode, etc.).
- Select the Tables node to display a list of tables.
- Select a table node to display the subordinate nodes.

Each of these can be selected to drill down for further information.

Note: *The User node displays the users who are permitted to access the table and what access permissions each user has.*

3.3.4. Create a New View

This procedure is used to create a new view definition.

- Select the Views node for the database.
- Select Create View from the context menu.

See "View Builder" in Section 2, "User Interface," for detailed instructions on view builder.

3.3.5. Modify a View Definition

A view can be modified only if it was originally created by the View Builder. These views are signified by the or icons. Select the view and then select Modify from the context menu. This invokes the interactive View Builder with that view loaded.

3.3.6. Re-create a View

When a database is remapped, all views are dropped from the relational catalog. View definitions created using the interactive view builder are retained in its own storage area. These views can be replayed to put them back in the relational catalog.

To replay a single view, select the view (it is designated by the icon) and select Replay View from the context menu.

To replay all views for the database, select the Views node and select Replay Views from the context menu.

3.3.7. Create a New Synonym

This procedure is used to create a new synonym for a table. It applies to relational tables only. Synonyms are useful in order to avoid having to qualify table names by their owner name. When you map a database, you can specify that public synonyms are created for each table.

- Select the table for which you want to create a synonym.
- Select Create Synonym from the context menu.
- Supply a legitimate SQL name by which this table will be known (the synonym name).

3.3.8. Change Access Permissions

See "Table/Users Node" in Section 2, "User Interface," for a description of how to change table or view access permissions.

3.4. User Procedures

This section describes procedures that relate to the administration of ODBC Access users.

3.4.1. Add a New User

This procedure is followed when a new user must use ODBC Access.

When using Windows authentication (the authentication for the default user is set to Windows), ensure that only the user name exists in the Windows domain. It is not necessary to perform any activity using the Administrator unless additional permissions must be granted for specific tables.

For other authentication methods, refer to the *ODBC Access Installation and Operations Guide* and the instructions for the All Users node in "User Interface" section in this guide.

3.4.2. Make a User the Default User

Parameters from the default user are used whenever the system automatically creates a user record. This takes place when the authentication method, as specified on the default user record, is Windows and there is not already a user record for that user. The parameters transferred from the default user to the new user are those that appear in the default user's Static tab under the All Users node. Permissions are not transferred.

Any user record can be designated the default user, but there might only be one. The default user record can be used to connect to the system, just like any other user record.

The current default user is marked with the icon.

- Select the user node you want to make the default user. It must be a user listed under the All Users node.
- Select Make user default from the context menu.

3.4.3. Set the System's Default Authentication Method

The default authentication method for the system is the authentication method defined for the default user. There are two ways to change it.

- Change the default user to one that has a different authentication method.
- Change the authentication method of the existing default user.

To set the default authentication for the system, perform the following steps:

- Select the default user node. It is marked with the icon.
- On the Static tab, change the Security Type.
- Choose Update.

3.4.4. Set Default Query Limits

The query limits set for the default user become the query limits for each user record that is automatically added to the system. To set them, do the following:

- Select the default user node. It is marked with the icon.
- On the Static tab, change the Limits as described in the instructions for the node in the section, "User Interface".
- Choose Update.

3.4.5. Monitor an Active User

Each time a user connects to a database through ODBC Access, an entry is created with the user name and a process or session number under the Active Users node. Select one of these nodes to view the user's current query progress relative to their query limits.

3.4.6. Stop a Runaway Query

With a judicious use of default query limits, there should not be any unreasonably long queries. However, if this situation does occur, the following procedure can be used to stop the query:

- Select the affected user under the Active Users node.
- Choose the Kill button in the right-hand pane.

The user receives an error message and can then submit another query. The session is retained.

Note: *The query is terminated as soon as there is network traffic between the ODBC Access SQL Server and the OS 2200 environment. In most cases, this causes the query to stop immediately. When processing push-down predicates, however, the components on the OS 2200 system might run for an extended period before responding.*

Appendix A
Troubleshooting

A.1. Overview

This appendix provides information on where to find information regarding known problems and how to obtain product support.

A.1.1. Electronic Support Services

Electronic Support Services, an online technical resource, is available to all Unisys customers with a service agreement. This information is available through the World Wide Web (WWW). Your maintenance contract entitles you to access the Unisys Support Online Web address:

http://www.service.unisys.com

This electronic service is available 24 hours a day, 7 days a week. It offers a wealth of technical information about Unisys hardware and software systems. Take some time to explore Unisys Support Online and discover the other electronic services available.

Use INFOACCESS to identify the ODBC Access for ClearPath OS 2200 Systems family of products when requesting information from the Unisys World Wide Web.

A.1.2. Unisys Support Center

If you have a problem that requires Unisys customer support, your site administrator should call the Unisys Support Center. The site administrator can also contact the Unisys Support Center through a Customer Assistance Request (CAR) on the WWW, using the Unisys Support Online Web address.

If a site administrator is not available, contact Unisys electronically at Unisys Support Online. If you are a client within the continental United States or Canada, call the toll-free number 24 hours a day, 7 days a week:

1-800-328-0440	United States
1-800-387-6181	Canada
1-800-361-8097	French Canada

If you are a client outside the continental United States or Canada, you can obtain a support center number from your local subsidiary.

A.1.3. Providing Information to Technical Support

Please have the following information available when contacting support:

- Your customer number
- The operating system and service pack level of the Windows server and the client system
- The version of all ODBC Access components that are installed
- The level of the ODBC Access driver installed on the PC
- A detailed description of the problem

Depending on the nature of your problem, technical support might also require the following:

- A copy of the Network Database Server schema source code
- A copy of the generated DDL. It can be found in the DDL folder within the ODBC Access Windows Server installation folder
- Contents of the config.ini file on the Windows client that has the problem
- Contents of the environment file
- Contents of the config.ini file from the Windows Server
- Traces as requested

Appendix B
Taking Traces

B.1. Overview

If the Administrator is not behaving as expected and the cause of the anomaly is not readily apparent to an ODBC Access support technician, you might be asked to take one or more traces and to send them to your Unisys support center. You should never need to take any traces unless specifically instructed to do so by support personnel, and then you should only take the requested traces. ODBC Access information is designed to aid technical support personnel. It is unlikely that trace information is meaningful to other parties.

B.2. Administrator Trace

Administrator tracing should not be turned on unless you are specifically directed to do so by technical support. Trace output normally occurs in three trace files, which are all located in the Administrator's Config folder. The default location for the Config folder is within the Administrator's installation folder. The files are

- Trace.txt
- Comserver_trace.txt
- UserInterface_trace.txt

All three of these files should be sent to technical support for analysis. It is possible that some scenarios are not generated in all three files. If that happens, only the generated ones should be sent to technical support.

Tracing is activated in the registry with the following procedure:

1. Select Run from the Start Menu, enter RegEdit, and choose OK.
2. Select the following key:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Unisys\Data Access\Administrator\
   ```

3. Find the numbered key that contains a value labeled "Install", which has a value corresponding to the path of the ODBC Access installation.

4. If there is no value labeled “Trace”, then right-click in the right-hand pane and select New, then String Value from the context menu. Set its name to Trace.
5. Double-click the “Trace” value and set its “Value data” to “Y”.
6. Perform the procedure that is traced.
7. Double-click the ”Trace” value and set its “Value data” to “N”.

Index

A

access mode, 2-21
action dialog, 2-11
active users node, 2-29
adding
  columns, 2-14
  new users, 2-22
  OS hosts, 2-18
  tables, 2-13
administrator trace, B-1
all users node, 2-22
  adding new users, 2-22
  disabled, 2-23
  limits I/O, 2-24
  limits rows, 2-24
  limits seconds, 2-24
  Max Bad Logons, 2-23
  name, 2-22
  password, 2-23
  removing users, 2-24
  security type, 2-24
  setting default user, 2-24
apply script, 2-3
authentication
  Data Access, 2-21
  default, 3-6
  preauthorized, 2-21
  Windows, 2-21

C

change access permissions, 3-5
changing column names, 2-14
changing table names, 2-13
changing user access, 2-15
changing views, 2-17
client service, 2-19
close database, 2-3
columns node, 2-13
  adding columns, 2-14
  changing column names, 2-14
  common procedures, 3-1
configuration node, 2-19
  access mode, 2-21
  client service, 2-19
  host name, 2-20
  log level, 2-20
  overview, 2-19
  port name, 2-20
  product key, 2-20
  RPC debug, 2-20
  select character set, 2-19
  server service, 2-20
  TC/IP address, 2-20
  TC/IP service, 2-20
configuration procedures, 3-1, 3-2
configuration, replacing lost, 3-2
connecting databases, 2-10
create view, 2-3, 3-4
creating new views, 2-17
creating synonyms, 2-3, 2-5, 2-18
creating synonyms, 3-5
creating view, 2-5

D

Data Access security, 2-26
  active users node, 2-29
  dynamic tab, 2-29
  preauthorized, 2-28
  Windows (do not impersonate), 2-27
  Windows (impersonate), 2-26
  Windows advanced options, 2-28
database admin menu, 2-2
  apply script, 2-3
  close database, 2-3
  create view, 2-3
  creating synonyms, 2-3
  drop synonym, 2-3
  drop view, 2-3
  grant permissions, 2-3
  new database, 2-2
  remap database, 2-3
  removing database, 2-2

database procedures, 3-1, 3-3
database status, 2-9
databases
  catalog loading, 3-3
  reload, 3-3
databases node, 2-9
  action dialog, 2-11
  connecting, 2-10
  depart after commit, 2-10
  external script, 2-11
  IAConnectTest, 2-9
  loading catalog, 2-10
  ODBC Access, 2-10
  open all areas, 2-10
  overview, 2-9
  reload, 2-11
  removing, 2-12
  status, 2-9
  updating database definitions, 2-11
DCOM, 1-2
default authentication, 3-6
default limits, 3-6
default users, 2-4, 3-5
definitions
  view table, 3-4
depart after commit, 2-10
disabled, 2-23
document conventions, 1-1
drop synonym, 2-3
drop view, 2-3
dynamic tab, 2-29
  kill, 2-29
  limits, 2-29

E

Electronic Support Services, A-1
exit, 2-1

F

file menu
  exit, 2-1
  save, 2-1

G

grant permissions, 2-3

H

host admin menu, 2-2
  new host, 2-2
  removing host, 2-2
host name, 2-20

I

IAConnectTest database, 2-9
indicies node, 2-14
installation, 1-4
installations node, 2-8
  service status, 2-8
Internet Explorer, 1-2

K

kill query, 2-29

L

limits, 2-29
  default, 3-6
  I/O, 2-24
  rows, 2-24
  seconds, 2-24
loading catalog, 2-10
local server account, 2-28
log level, 2-20

M

Max Bad Logons, 2-23
modify, 2-5
modify view, 3-4
monitor users, 3-6
msvcrt.dll, 1-3

N

new, 2-5
new database, 2-2
new host, 2-2
new server, 2-2
new users, 2-4

new users, 3-5

O

ODBC Access, 2-10
ODBC Access node, 2-6
ODBC infrastructure, 1-2
open all areas, 2-10, 2-12
OS 2200 host, adding, 3-2
OS host, 2-12, 2-18
  adding, 2-18
  overview, 2-18
  removing, 2-19

P

password, 2-8, 2-23
permissions, 1-5
  change access, 3-5
port name, 2-20
preauthorized, 2-28
procedures
  common, 3-1
  configuration, 3-1, 3-2
  database, 3-1, 3-3
  user, 3-1, 3-5
product description, 1-3
product key, 2-20
properties, 2-2

R

re-creating views, 2-17, 3-4
refresh, 2-2, 2-5
reload, 2-11
remap database, 2-3
removing, 2-5
  database, 2-2
  databases, 2-12
  host, 2-2
  hosts, 2-19
  server, 2-2
  synonyms, 2-18
  user, 2-4
  user access, 2-15
  users, 2-24
  views, 2-17
replay view, 2-5
RPC debug, 2-20
runaway query, 3-7

S

save, 2-1, 2-4
security types, 2-24, 2-25
  Data Access security, 2-26
select character set, 2-19
server admin menu, 2-2
  new server, 2-2
  removing server, 2-2
server domain, 2-28
server service, 2-20
servers node, 2-6
  adding, 2-7
  overview, 2-6
  removing, 2-7
setting default user, 2-24
setting table permissions, 2-13
synonym, create, 3-5
synonyms node, 2-17
  creating, 2-18
  overview, 2-17
  removing, 2-18
system requirements
  DCOM, 1-2
  Internet Explorer, 1-2
  msvcrt.dll, 1-3
  ODBC infrastructure, 1-2
SysUsers, 2-1

T

tables node, 2-12, 2-14
  adding tables, 2-13
  changing names, 2-13
  changing user access, 2-15
  overview, 2-14
  removing user access, 2-15
  setting permissions, 2-13
  unexpected behavior, 2-15
TCP/IP
  address, 2-20
  host, 2-12, 2-18
  service, 2-18, 2-20
tool bar
  creating synonym, 2-5
  creating view, 2-5
  modify, 2-5
  new, 2-5

refresh, 2-5
removing, 2-5
replay view, 2-5
save, 2-4
trace
administrator, B-1
tree view, 2-6
all users node, 2-22
columns node, 2-13
configuration node, 2-19
databases node, 2-9
indicies node, 2-14
installations node, 2-8
ODBC Access node, 2-6
OS host, 2-12, 2-18
servers node, 2-6
synonyms node, 2-17
tables node, 2-12, 2-14
users node, 2-14, 2-21
views node, 2-16
troubleshooting, A-1
trusted domains, 2-28

U

UDS slots, 2-12
UNC, 2-11
Unisys Support Center, A-1
updating database definitions, 2-11
user admin menu, 2-4
default user, 2-4
new users, 2-4
removing user, 2-4
user interface
menus, 2-1
overview, 2-1
security types, 2-25
tool bar, 2-4
tree view, 2-6
View Builder, 2-30
user procedures, 3-1, 3-5
users
default, 3-5
limits I/O, 2-24
limits rows, 2-24
limits seconds, 2-24
monitor, 3-6
new, 3-5
runaway query, 3-7
users name, 2-22
users node, 2-14, 2-21
changing user access, 2-15
overview, 2-14, 2-21
removing user access, 2-15
unexpected behavior, 2-15

V

view
create, 3-4
modify, 3-4
recreating, 3-4
view builder
select columns, 2-31
select conditions, 2-34
select expressions, 2-31
select tables, 2-31
setup column expression, 2-32
setup conditions, 2-33
view name, 2-30
View Builder, 2-30
view menu, 2-2
properties, 2-2
refresh, 2-2
view table definitions, 3-4
view users, 2-17
viewing remote databases, 1-5
views node, 2-16
changing, 2-17
creating new views, 2-17
overview, 2-16
recreating, 2-17
removing, 2-17
view users, 2-17

W

Windows
do not impersonate, 2-27
domain, 2-28
impersonate, 2-26
server, 3-2
Windows advanced options, 2-28
local server account, 2-28
server domain, 2-28
trusted domains, 2-28
Windows service, 2-8
start, 2-8
stop, 2-8

© 2013 Unisys Corporation.
All rights reserved.

7862 5746–004